This chapter implements STANAG 2844 (Edition Two)

Chapter 1

MISSION AND STRUCTURE

GENERAL

Threat intelligence services have the capability to conduct continuous collection against the US Army during peacetime, operations other than war (OOTW), and during war itself. The intelligence that results from these operations provides a significant advantage to threat forces, and could easily result in increased US casualties on the battlefield. Fortunately, there are many actions we can take to counter threat intelligence efforts and to provide force protection to all US Army units.

The most dramatic of these actions are designed to neutralize enemy collection. These actions include—

- Using field artillery to destroy ground-based enemy signals intelligence (SIGINT) collectors.
- Conducting sophisticated C-HUMINT operations in a foreign city long before overt hostilities commence.
- Employing direct fire weapon systems to destroy enemy reconnaissance. Brigades conducting defensive operations at the National Training Center often commit a tank-infantry company team to provide counterreconnaissance, intelligence, surveillance, and target acquisition (C-RISTA) protection.

While not as flashy, routine security procedures provide crucial force protection. These procedures include but are not limited to—

- Personnel security, to include background investigations, will ensure all personnel who have access to sensitive or classified information will fully protect it.
- Information security, particularly in regard to handling classified and compartmented information, will be a challenging field in the future considering the ease with which information can be copied and transmitted in an increasingly automated Army.

- Physical security, which ensures physical measures are taken to safeguard personnel, prevents unauthorized access to equipment, installations, materiel, and documents to safeguard them against espionage, sabotage, damage, and theft.

- Operations security (OPSEC), which ensures that all essential elements of friendly information (EEFI), are reasonably concealed from enemy collection assets.

Another crucial component in the fight against threat collection efforts is CI analysis. These include efforts to identify the general capabilities and specific operations of enemy human intelligence (HUMINT), SIGINT, and imagery intelligence (IMINT) collection. CI analysis also includes the development of profiles that identify friendly vulnerabilities to enemy collection and possible countermeasures.

Measures such as these provide a crucial force protection shield that is difficult for the FIS to penetrate. More importantly, a comprehensive CI program significantly degrades the threat's ability to target and conduct combat or terrorist operations against US Forces. Total CI provides the combat commander with a definite advantage on the battlefield.

AR 381-10, AR 381-12, and AR 381-47 (S) contain policies and procedures governing the conduct of intelligence activities by Department of the Army (DA).

MISSION

The CI mission is authorized by Executive Order (EO)12333, implemented by AR 381-20. The Army conducts aggressive, comprehensive, and coordinated CI activities worldwide. The purpose is to detect, identify, assess, counter, neutralize, or exploit threat intelligence collection efforts. This mission is accomplished during peacetime and all levels of conflict. Many CI functions, shown in Figure 1-1, are conducted by echelons above corps (EAC); some by echelons corps and below (ECB); and some are conducted by both. Those CI assets found at ECB respond to tactical commanders. EAC assets respond primarily to commanders of intelligence units while supporting all commanders within their theater or area of operations (AO).

CI FUNCTION	EAC			ECB		
	PEACE	WAR	OOTW	PEACE	WAR	OOTW
INVESTIGATIONS						
Personnel Security (OCONUS)	X	X	X	X	X	X
Army CI Investigations:						
Treason	X	X	X		X	
Espionage	X	X	X	X	X	X
Spying		X	X			
Subversion		X				
Sedition		X				
FIS-directed sabotage	X	X	X	X	X	X
Terrorism	X	X	X	X	X	X
Assassination	X	X	X	X	X	X
Defection	X	X	X	X	X	X
Detention	X	X	X	X	X	X
Special category absentees	X	X	X	X	X	X
Deliberate security violations	X	X	X	X	X	X
Suicide or attempted suicide	X	X	X	X	X	X
CI scope polygraph examinations	X	X	X			
Technical penetration	X	X	X			
OPERATIONS						
CI special operations (AR 381-47 (S))	X	X	X			
CI support to force protection:	X	X	X	X	X	X
CI support to mobilization	X	X	X	X	X	X
CI support to combatting terrorism	X	X	X	X	X	X
CI support to rear operations		X	X		X	X
CI support to civil-military operations		X	X		X	X
CI support to psychological operations		X	X		X	X
CI support to battlefield deception		X	X		X	X
CI support to OPSEC	X	X	X	X	X	X
CI support to friendly C-E	X	X	X	X	X	X
CI support to information operations	X	X	X	X	X	X
CI support to counter-drugs	X		X	X		X
CI force protection source operations (deployed)	X	X	X	X	X	X
Advice and assistance	X	X	X	X	X	X
CI technical support activities	X	X	X			
CI support to acquisition and SAPs	X	X	X			
CI support to HUMINT	X	X	X			
CI support to treaty verification	X	X	X	X		X
Liaison	X	X	X	X	X	X
CI support to domestic civil disturbance			X			X
CI support to natural disaster operations			X			X
C-SIGINT support	X	X	X	X	X	X
C-IMINT	X	X	X	X	X	X
Hostile intelligence simulation (Red Team)	X	X	X			
Covering agent support	X	X	X	X	X	X
COLLECTION						
Identifying and validating requirements	X	X	X	X	X	X
Local operational data collection	X	X	X	X	X	X
Debriefing and interrogation	X	X	X	X	X	X
Returned US defector debriefing	X	X	X	X		X
ANALYSIS AND SYNTHESIS						
Threat and friendly databases	X	X	X	X	X	X
Threat assessment	X	X	X	X	X	X
Vulnerability assessment	X	X	X	X	X	X
Countermeasures recommendations	X	X	X	X	X	X
Countermeasures evaluation	X	X	X	X	X	X

Figure 1-1. Counterintelligence functions.

The essence of the Army's CI mission is to support force protection. By its nature, CI is a multidiscipline (C-HUMINT, C-SIGINT, and C-IMINT) function designed to degrade threat intelligence and targeting capabilities. Multidiscipline counterintelligence (MDCI) is an integral and equal part of intelligence and electronic warfare (IEW). MDCI operations support force protection through OPSEC, deception, and rear area operations across the range of military operations. For more information on IEW operations, see FM 34-1.

CI IN SUPPORT OF FORCE XXI

CI must meet the goals and objectives of Force XXI and force projection operations. US Forces will be continental United States (CONUS)-based with a limited forward presence. The Army must be capable of rapidly deploying anywhere in the world; operating in a joint or combined (multinational) environment; and defeating simultaneous regional threats on the battlefield; or conducting OOTW. CI, as part of IEW, is fundamental to effective planning, security, and execution of force projection operations. Successful force projection CI support is based on the same five key principles shown in Figure 1-2 and discussed below. CI, in support of force protection, will be required on the initial deployment of any force projection operation.

THE COMMANDER DRIVES INTELLIGENCE:
The commander focuses on the intelligence system by clearly designating his priority intelligence requirements (PIR), targeting requirements and priorities. He ensures that the Intelligence Battlefield Operating System (BOS) is fully employed and synchronized with his maneuver and fire support BOSs. He demands that the Intelligence BOS provides the intelligence he needs, when he needs it, and in the form he needs.

INTELLIGENCE SYNCHRONIZATION:
The J2 or G2 synchronizes intelligence collection, analysis, and dissemination with operations to ensure the commander receives the intelligence he needs, in the form he can use, and in time to influence the decisionmaking process. Intelligence synchronization is a continuous process which keeps IEW operations tied to the commander's critical decisions and concept of operations. CI collection, analysis, and dissemination, like other intelligence, have to meet the commander's time requirements to be of any use other than historical.

SPLIT-BASED OPERATIONS:
Split-based operations provide deploying tactical commanders with a portion of their collection assets and augment full employment of organic

assets. Split-based intelligence operations employ collection and analysis elements from all echelons, national to tactical, in sanctuaries from which they can operate against the target area.

TACTICAL TAILORING:

In force projection operations, the commander tactically tailors CI, as well as all IEW, support for each contingency based on the mission and availability of resources. He must decide which key CI personnel and equipment to deploy early, and when to phase in his remaining CI assets.

BROADCAST DISSEMINATION:

Broadcast dissemination of intelligence includes the simultaneous broadcast of near-real time (NRT) CI from collectors and processors at all echelons. It permits commanders at all echelons to simultaneously receive the same intelligence, thereby providing a common picture of the battlefield. It allows commanders to skip echelons and pull CI directly from the echelon broadcasting it.

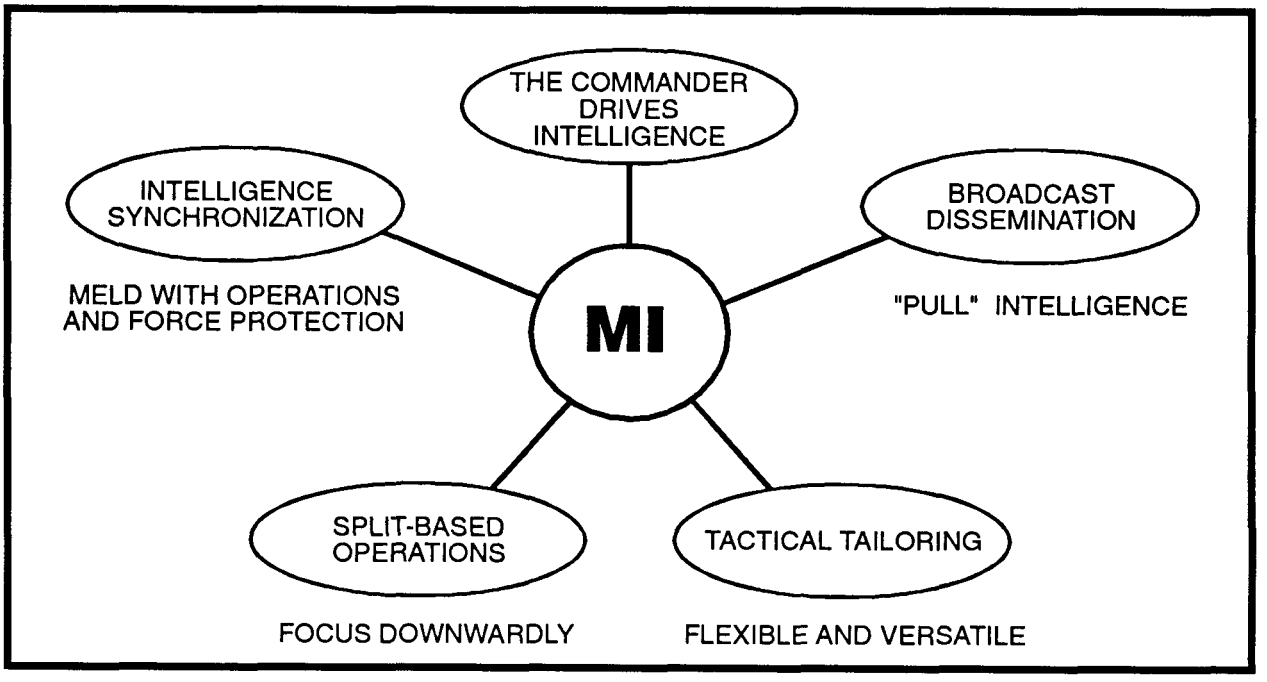

Figure 1-2. Principles of force projection IEW operations.

INTELLIGENCE TASKS

Army military intelligence (MI) accomplishes its mission by performing six primary tasks: providing indications and warnings (I&W); performing intelligence preparation of the battlefield (IPB); performing situation development; supporting target development and targeting; developing force protection intelligence; and performing battle damage assessment (BDA).

CI TASKS

The role of CI is to support the commander's requirements to preserve essential secrecy and to protect the force directly or indirectly. Thus, CI contributes to the commander's force protection programs. Force protection is a command responsibility to protect personnel, equipment, and facilities. To carry out his force protection responsibilities, a commander requires support from several sources, one of which is the intelligence community. CI support to force protection must be tailored to the sensitivity of the supported organization and its vulnerability to FIS and hostile attack. CI support can be tailored from a combination of activities to include—

- Mobilization security, including ports and major records repositories.
- Combatting terrorism.
- Rear operations.
- Civil-military affairs.
- Psychological operations (PSYOP).
- Battlefield deception.
- OPSEC.
- Friendly Communications-Electronics (C-E) (C-SIGINT).
- CI force protection source operations (CFSO).

ARMY CI AS A FUNCTION OF MI

Army CI, as a multidiscipline intelligence function, is an integral part of the Army and Department of Defense (DOD) and national intelligence communities. CI missions are conducted in support of the objectives of these communities.

COUNTERRECONNAISSANCE

CI is an integral part of the command counterreconnaissance effort. Human and other intelligence sensors determine adversary reconnaissance, intelligence, surveillance, and target acquisition (RISTA) and other battlefield capabilities, and project resultant data into battle planning and execution. As the adversary worries about our C-RISTA capability, our CI efforts target his RISTA capabilities. CI focuses on the HUMINT threat in the AO and provides analytical support in identifying enemy SIGINT and IMINT capabilities and intentions. CI has a limited neutralization and exploitation capability directed at low-level adversary HUMINT collectors or sympathizers acting in a collection or sabotage capacity. The commander is responsible for security countermeasure programs and training to include personnel, physical, document, information security, crime prevention, and OPSEC.

OTHER SPECIALTIES

Army CI is not limited to the activities of a small force of CI agents and technicians; rather, it is the responsibility of all Army personnel to follow common sense security measures to minimize any foreign intelligence threat.

Although a major part of the CI mission is to counter or neutralize FIS efforts, this does not mean that only CI personnel take part in these actions. They may require—

- Other intelligence specialists such as interrogators.
- Military police (MP).
- Civilian counterparts and authorities.
- Combat forces.
- Civil-military affairs and PSYOP.

- Criminal Investigation Command (CIDC) agents.

The combined use of C-HUMINT, C-SIGINT, and C-IMINT TTPs provides a multidisciplined approach to denying information to unauthorized persons. This approach limits the threat's ability to collect against us. Although this FM describes these three operations separately in Chapter 3, they are often conducted simultaneously by the same assets.

PEACE, WAR, AND OOTW

The Army conducts CI during peacetime and at all levels of conflict to protect the force from foreign exploitation. During peacetime, CI simultaneously supports the commander's needs and DA policy.

During war, CI operations are much the same as in peacetime, except the adversary state or nation is well-defined. The commander's needs are the top priority.

OOTW may include the direct or indirect support of one or more foreign governments or groups, or international organizations such as the North Atlantic Treaty Organization (NATO). OOTW may be initiated unilaterally in the absence of foreign support. Whether unilateral or multinational, US Forces usually operate in a joint environment. Normally in OOTW, military force is used only as a last resort. OOTW consists of the following operational categories:

- Noncombatant evacuation operations.
- Arms control.
- Support to domestic civil authorities.
- Humanitarian assistance (HA) and disaster relief.
- Security assistance.
- Nation assistance.
- Support to counter-drug operations.
- Combatting terrorism.
- Peacekeeping operations.

- Peace enforcement.
- Show of force.
- Support for insurgences and counterinsurgencies.
- Attacks and raids.

THE CI STRUCTURE

To accomplish the CI mission at various echelons, specially trained CI personnel are assigned to tactical CI organizations as shown in Figure 1-3. Organizations include—

- CI organizations organic to theater Army MI brigades or groups which are United States Army Intelligence and Security Command (INSCOM) organizations.
- Tactical exploitation battalion (TEB) and headquarters (HQ) and operations battalion of the corps MI brigade.
- MI battalion at division.
- MI companies at armored cavalry regiments (ACRs) and separate brigades.
- MI elements at special forces groups.

At each echelon, CI teams provide command and control (C^2) of CI assets; conduct CI investigations, operations, and collection; perform analysis and produce CI products; and provide security advice and assistance.

Only CI officers, technicians, agents, or accredited civilian employees control and conduct investigations. Additionally, DA policy identifies CFSO as a CI function as described in Chapter 4. CI personnel are also collectors of information, working individually or in teams with interrogators and technicians when resources permit. At ECB, CI personnel work in CI platoons at division level and CI companies at corps level. At EAC, CI personnel work individually or in groups in field offices, resident offices, or MI detachments or companies.

Another CI military occupational specialty (MOS) is MDCI analyst 97G. In addition to performing C-SIGINT operations and communications monitoring, these soldiers perform MDCI analysis and produce MDCI products.

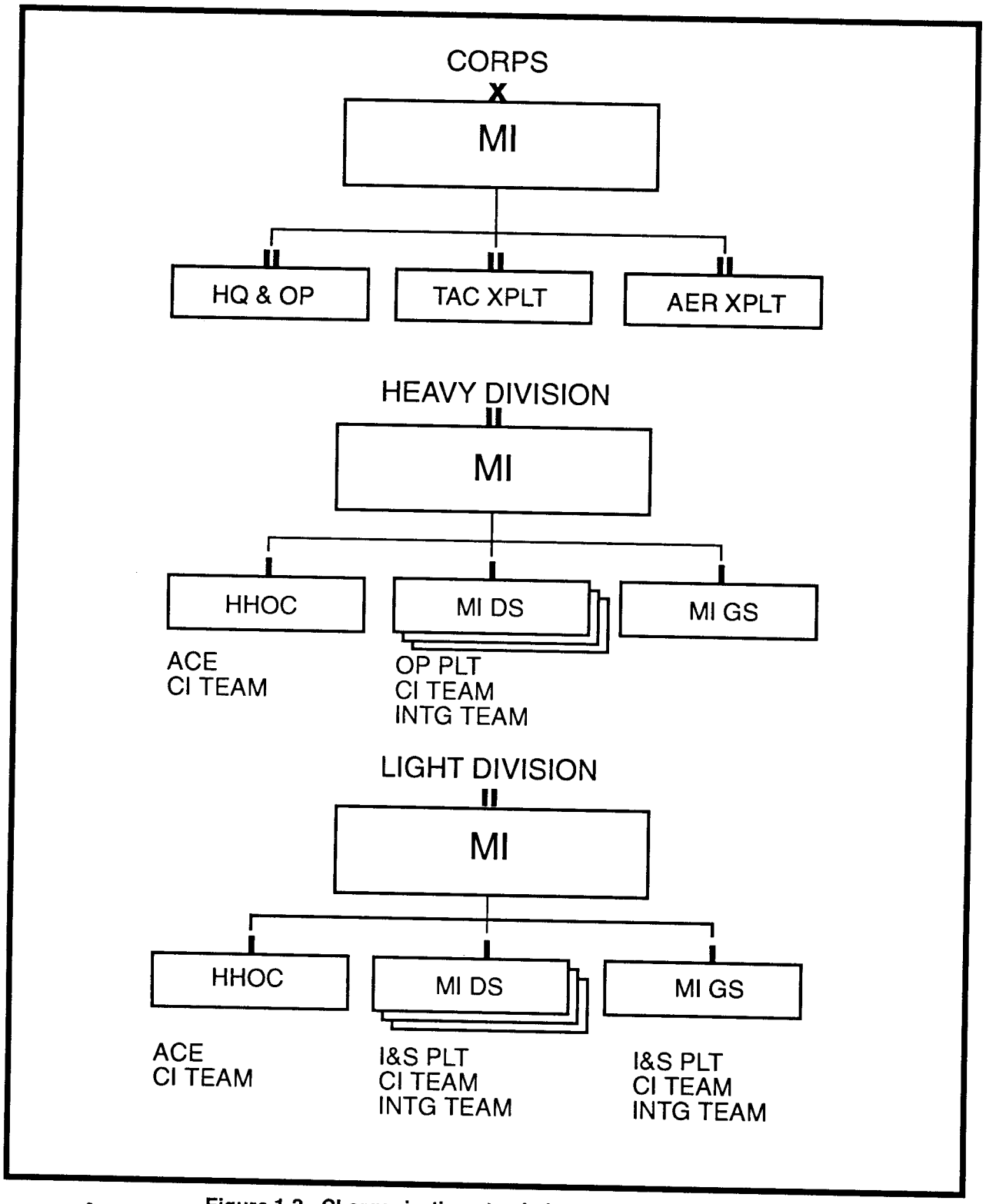

Figure 1-3. CI organization at echelons corps and below.

Interrogator and other personnel possessing requisite linguistics capability work with CI teams when conditions and resources permit. Provided these personnel are competent in the foreign language appropriate to the AO and possess the required security clearance, they perform interpreter, translator, liaison officer, and (after appropriate training) source handler duties.

CI teams, found in some tactical units, are task organized based on mission, enemy, troops, terrain and weather, and time available (METT-T) factors. CI teams are composed of a CI technician, several CI agents and interrogation personnel, and MDCI analysts. Other CI teams are composed of CI agents and analyst personnel. At EAC, CI personnel work individually or in groups in resident offices, field offices, MI detachments, companies, or regions. Depending on the mission, additional specialists may either be attached or task organized to provide temporary expertise, such as—

- Physical security specialists.
- MP.
- Other intelligence personnel trained to accomplish a specific mission.

CI SUPPORT TO US FORCES

CI assets are deployed to provide area coverage. Only when driven by PIR should they be given a mission other than area coverage, such as specialized support to a special access program. When assigning missions to CI elements, METT-T must be carefully considered to ensure tasks are prioritized and CI assets are properly utilized.

Most CI operations develop slowly. Therefore, missions should be assigned for relatively long periods. If a team is investigating a sabotage incident, its mission should be assigned for as long as it takes to complete the mission. If a team is establishing liaison with host nation officials, this mission should remain with the team long enough to turn the liaison over to another team.

Within corps and divisions, CI assets are given an area coverage role. Based on priorities established by the corps or division commander, or G2, the MI battalion commander controls the CI assets as they execute the mission.

Although CI operations may change with priorities, CI assets must attempt to ensure commanders get what they need, when they need it, and in a form they can use before changing missions.

PLANNING

For contingency operations, CI elements should have the following procedures firmly in place prior to deployment:

- Updated threat databases.
- Planned CI communications in time to support decisionmaking.
- Approved operations plans (OPLANS) with financial annexes for any source operations; for example, CFSO and host country liaison.
- Appropriate and up-to-date country studies.
- Established intelligence contingency funds (ICF). See AR 381-141.
- Ongoing contact with theater CI elements to facilitate exchanging information and, where applicable, passing assets after employment.
- Team reaction time must be rapid since contingencies can occur in locations with no US presence and with little warning. Therefore, the team needs a good working relationship with elements maintaining CI databases. The team should have a generic plan or established standing operating procedures (SOPs) which vary according to the type of OOTW. Teams would not do exactly the same things in peacekeeping, peace enforcement, and CI support to treaty verification, domestic civil disturbances, and natural disaster operations. Generally, the team must consider what is appropriate and feasible.
- Procedures which tailor intelligence support packages to support planning and contingency operations should refer to the National Ground Intelligence Center (NGIC) and the 902d MI Group CI Analysis Center (CIAC) as a source of data.

TASKING AND REPORTING

CI teams receive taskings based on requirements from higher echelon. Taskings are normally generated by collection managers based on command needs or information gaps in analytical holdings and provided to the commander of the CI assets. CI teams also request information from organizations (such as HUMINT, SIGINT, or IMINT collectors) in support of CI missions.

Units report information based on the mission assigned and information collected. Information is reported to the CI unit's parent unit for C*. It is also reported to others as directed by the parent unit, depending on the situation, mission, and the type and sensitivity of information collected. Other recipients of information could include—

- Theater J2 or Joint Task Force CI Coordinating Authority (JTFCICA), if applicable.
- G2 or Deputy Chief of Staff, Intelligence (DCSINT) of theater ground component commander.
- Other units, as appropriate, approved by the Ml unit commander.

JOINT AND COMBINED OPERATIONS

Any future conflict may involve joint and combined operations. See FM 34-1. While operational control of intelligence elements normally rests with component commanders, joint staffs coordinate and provide operational guidance. In the case of CI operations, the J2, through the JTFCICA in accordance with Joint Publication 2-01.2, establishes areas of responsibility for CI operations for component forces; produces and disseminates CI products by integrating information provided by subordinate commands; and coordinates and obtains intelligence and CI support from national agencies and disseminates this information to operational commands.

JOINT OPERATIONS:

Most contingency operations require the deployment of joint forces. Deployment is directed by the national command authority. When this occurs, CI elements from various services (component commands of the joint command) may be included in the task organization. The joint force or task force commander and staff must either identify specific operational boundaries or combine CI assets under a common command. This ensures continuity of effort without duplication.

If the IEW organization does not include CI assets and CI assets are added from nonorganic organizations, they should be assigned under the operational control of the commander of the IEW organization. This clearly identifies C* relationships. For more information on IEW organization, see Joint Publication 2-01.2.

COMBINED OPERATIONS:

The US Army and its allies conduct combined CI operations to attain mutual objectives. In many cases they conduct these operations because the operating area does not permit Americans to conduct unilateral operations.

Combined operations are required by Status of Forces Agreements (SOFAs). In either case, the objective is the same—to counter the intelligence capabilities and operations of our adversaries. Combined CI operations include—

- Investigations.
- CI support to deception.
- CI support to OPSEC.
- CFSO.
- Security advice and assistance.
- CI analysis and production.

Combined CI operations range from a mere exchange of information to conducting integrated CI operations. Local policy and procedures dictate the extent to which combined operations are conducted.

SPECIAL OPERATIONS:

CI is a critical component of intelligence support to Army Special Operations Forces (ARSOF). There are CI and interrogation assets included in the organic structure of ARSOF units. CI elements conduct tactical HUMINT collection, analysis and production, and other operations support activities which include but are not limited to—

- CI support to OPSEC.
- CI support to deception.
- CI liaison.
- CFSO.
- Limited investigations.

CI support to ARSOF is conducted throughout the phases of force protection operations during peace, war, and OOTW and must be tailored. For more information on CI operations, see FM 34-5 (S).

LEGAL REVIEW

CI activities are authorized by law and regulation. Commanders and CI personnel should coordinate CI activities with the servicing judge advocate for verification of compliance with law and regulation prior to execution. Where appropriate, judge advocates should be part of the planning process.